RSA INCIDENT DISCOVERY AND RESPONSE SERVICES

Cyber Readiness, Response and Resilience

AT-A-GLANCE

The RSA® 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.

EXECUTIVE SUMMARY

The need for strong cyber security and threat management has never been greater than it is today. Public and private enterprises face a growing risk of compromise from hackers, targeted attack adversaries and fraudsters. Due to a reliance on security strategies and infrastructure implemented for yesterday's threats, organizations are unprepared to counteract the attacks designed specifically to undermine traditional security defense mechanisms.

The RSA® Incident Discovery, Incident Response Rapid Deploy and Incident Retainer services provide organizations with tactical insight into activities taking place on their systems. They also facilitate surge access to resources and expertise when anomalous activities are suspected or detected. Through the capture and analysis of live network traffic and host data using the award winning RSA Security Analytics platform and RSA ECAT, expert analysts review the overall state of the environment and identify areas of concern:

– Anomalous activities on network and host systems

– Adversary Tools, Tactics and Procedures

– Assets which may be targeted

Core focus areas when proactively searching for anomalies (Incident Discovery) and when responding to an incident (Incident Response Rapid Deploy) include:

– Threat Intelligence and malware analysis

– Network and Host-based forensic analysis

The combination of these components provides the basis for situational awareness. Analysis of information in any one domain can provide useful information, but it is the totality of the information that leads to successful incident response. This includes the ability to determine the scope of adversary activities and make informed tactical decisions in a timely manner. With the preservation of all potential sources of evidence and visibility and context across the enterprise, an organization can develop a program for remediation and incident management.

SOLUTION PORTFOLIO

RSA's broad portfolio of solutions enables organizations to formulate the strategy and tactics for Advanced Cyber Defense. The combination of services and technology provides an agile platform for the design of a risk intelligent operation that suits a wide range of security postures and risk propensity levels.

RSA SOLUTIONS FOR ADVANCED CYBER DEFENSE

- Advanced SOC Design & Implementation
- Security Operations Management
- Vulnerability & Risk Management
- Cyber & Counter Threat Intelligence
- Incident Response
- Security Strategy & Program Development

Readiness, Response & Resilience

TAKE THE NEXT STEP

To benefit from RSA's Incident Discovery, Incident Response Rapid Deploy and Incident Retainer services, please contact your RSA services sales representative.

ABOUT RSA

RSA, The Security Division of EMC, is the premier provider of security, risk and compliance management solutions for business acceleration. RSA helps the world's leading organizations succeed by solving their most complex and sensitive security challenges. These challenges include managing organizational risk, safeguarding mobile access and collaboration, proving compliance, and securing virtual and cloud environments.

Combining business-critical controls in identity assurance, encryption & key management, SIEM, Data Loss Prevention and Fraud Protection with industry leading eGRC capabilities and robust consulting services, RSA brings visibility and trust to millions of user identities, the transactions that they perform and the data that is generated. For more information, please visit www.RSA.com and www.EMC.com.

RSA