RSA® MALWARE INTELLIGENCE PROGRAM FOR ECAT

Malware Detection and Analysis to Protect Critical Assets

AT-A-GLANCE

- End-to-end solution for malware detection and analysis
- Focus on business priorities and the need to safeguard the organizational mission
- Alignment with requirements and capabilities for closed-loop incident handling
- Technical proficiency and expertise to expedite time-to-value with RSA ECAT

EXECUTIVE SUMMARY

Organizations have been dealing with targeted attacks and Advanced Threats for over ten years. Recently, these attacks have gained more publicity as the threat has become more pronounced and as breaches involving global brand names have been disclosed. Yet security defenses still rely on "known bad" mechanisms such as malware signatures and other known Indicators of Compromise. This leaves the organization exposed to zero-day vulnerabilities where "known bad" indicators do not exist. RSA ECAT uses a different approach. It conducts live memory and behavioral analysis and assigns a suspect level score to each application module. By applying intelligence to whitelist "known good" modules the security analyst is able to focus on advanced and unknown threats and anomalies. By adopting a signature-less approach to malware detection and analysis organizations can defend against targeted attacks for a more proactive security posture.

RSA Professional Services accelerates time-to-value by enabling organizations to rapidly leverage product investments, align use cases with business requirements and update standard operating procedures. The RSA Malware Intelligence Program for ECAT service addresses the lifecycle of requirements, from analysis and design to deployment and management.

This service facilitates and accelerates the development of an enterprise malware intelligence capability using ECAT to identify, collect and analyze the types of clues which targeted attacks leave behind thereby reducing Breach Exposure Time and protecting critical assets.

In association with this service, RSA's consultants address business and technical requirements and the operational model required to ensure a successful deployment. Key components include:

- Review of policies and procedures, use cases, roles and responsibilities to ensure that ECAT will meet business objectives
- Architecture & Design to optimize technical specifications and performance
- Integration with Threat Intelligence capabilities for proactive mitigation and prevention strategies

Benefits include a solution that is designed to protect the organizational mission by early threat detection and closed-loop incident handling. By utilizing a holistic approach to solution fulfillment RSA Professional Services can help organizations implement more effective counter-measures to deal with targeted attacks and Advanced Threats.
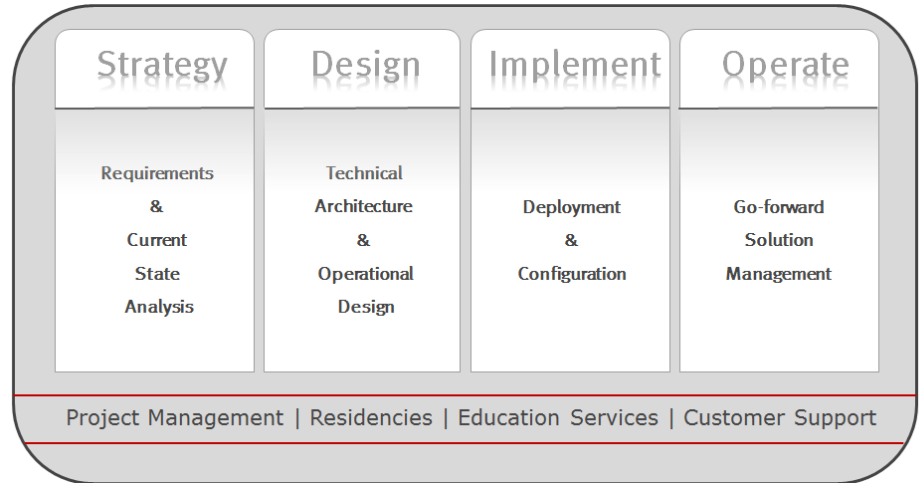
RSA®

EMC²®

SOLUTION FULFILLMENT

RSA's Service Delivery Framework addresses the Business, Operational and Technical requirements for holistic solution fulfillment and leverages the expertise that comes from thousands of engagements and over thirty years of industry leadership experience. As adversaries have grown more sophisticated, RSA's continued investment in new solutions can help organizations evolve with the changing threat landscape.

RSA SERVICE DELIVERY FRAMEWORK

Strategy	Design	Implement	Operate
Requirements & Current State Analysis	Technical Architecture & Operational Design	Deployment & Configuration	Go-forward Solution Management

Project Management | Residencies | Education Services | Customer Support

TAKE THE NEXT STEP

To benefit from the RSA Malware Intelligence Program for ECAT service, 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.

www.rsa.com

RSA®

EMC²®